UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA v. JUSTIN GRAY LIVERMAN (a/k/a "D3F4ULT") Defendant.	Criminal No. 1:16-cr-313 Honorable Gerald Bruce Lee Sentencing: July 28, 2017

GOVERNMENT'S POSITION ON SENTENCING

Defendant Justin Gray Liverman has pleaded guilty to conspiring with Andrew Otto Boggs[1] and others to commit (1) identity theft, (2) unauthorized access to a protected computer, and (3) anonymous and repeated telecommunications harassment. His conviction stems from his conduct in 2015 and 2016 with an online collective – calling itself "Crackas with Attitude" or CWA – that targeted U.S. government personnel for harassment and unauthorized account intrusions. The Presentence Investigation Report (PSR) calculates the defendant's total offense level as 25; with the defendant's criminal history category of 1, the resulting Guidelines range is 57-71 months' imprisonment. The statutory maximum term of imprisonment is 60 months. The government submits that under the factors in 18 U.S.C. § 3553(a), a sentence at the low end of this guidelines range would be sufficient but not more than necessary to meet the objectives in that statute. The government further requests that the Court order three years of supervised

[1] Case No. 1:16-CR-314-GBL (E.D. Va.). On June 30, 2017, Boggs was sentenced to 24 months' imprisonment and three years of supervised release. For the reasons explained herein, the Government believes that Liverman's sentence should be significantly more than the 24 months' imprisonment received by Boggs to reflect his greater role in the conspiracy.

release and full restitution that imposes joint and several liability on co-conspirator Boggs, who was sentenced on June 30, 2017.

SENTENCING ANALYSIS

Earlier this year, defendant pleaded guilty to one count of conspiracy to commit (1) identity theft (a violation of 18 U.S.C. § 1028), (2) unauthorized access to a protected computer (a violation of 18 U.S.C. § 1030), and anonymous and repeated telecommunications harassment (a violation of 47 U.S.C. § 223(a)), all in violation of 18 U.S.C. § 371. PSR ¶ 4. The maximum penalties for this crime are 5 years' imprisonment, a $250,000 fine, and 3 years of supervised release. Defendant has also agreed to pay full restitution and a $100 special assessment. A forfeiture order was entered at defendant's plea hearing.

The Sentencing Guidelines and the factors in 18 U.S.C. § 3553(a) govern the Court's sentencing analysis. While the Guidelines have been advisory since 2005, district courts are required to "consult those Guidelines and take them into account when sentencing." *United States v. Booker*, 543 U.S. 220, 264 (2005). Indeed, the continued use of the Guidelines as a benchmark helps to avoid unwarranted sentencing disparities. After calculating the appropriate sentencing range, "the court shall consider that range as well as other relevant factors set forth in the guidelines and those factors set forth in [18 U.S.C.] § 3553(a) before imposing the sentence." *United States v. Hughes*, 401 F.3d 540, 546 (4th Cir. 2005) (citation omitted).

I. Sentencing Guidelines

The plea agreement in this case stipulates that the following provisions of the Guidelines apply:

a. Section 1B1.2(d) and 2X1.1 apply to defendant's conviction;

b. For the conspiracy object to violate 47 U.S.C. § 223, U.S.S.G. § 2A6.1 governs;

c. For the conspiracy objects to violate 18 U.S.C. §§ 1030 and 1028:

   i. The base offense level, established in U.S.S.G. § 2B1.1, is 6;

   ii. The loss amount for the conspiracy is more than $1.5 million but not more than $3.5 million, and the loss amount attributable to defendant under 18 U.S.C. § 3664(h) is at least more than $95,000 for purposes of U.S.S.G. § 2B1.1(b)(1);

   iii. Because a substantial part of a fraudulent scheme was committed from outside the United States, and the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means, the offense level must be increased by an additional 2 levels under U.S.S.G. § 2B1.1(b)(10); and

   iv. Because a victim was a government officer or employee, or a former government officer or employee, and the offense of conviction was

motivated by such status, the offense level must be increased by an additional 3 levels under U.S.S.G. § 3A1.2(a).

d. The defendant has assisted the government in the investigation and prosecution of the defendant's own misconduct by timely notifying authorities of the defendant's intention to enter a plea of guilty, thus the offense level must be decreased by 2 levels under U.S.S.G. § 3E1.1.

In the PSR, the Probation Office computed offense levels for the five individual victims as well as the agencies. PSR ¶¶ 52-101. For the five individual victims, the PSR calculated the base offense level as 12 pursuant to U.S.S.G. § 2A6.1(a)(1). For the five individual victims, the PSR also included a 2-level increase pursuant to U.S.S.G. § 2A6.1(b)(2)(A) because the offense involved more than two threats. For Victims 1 and 2, the PSR included a 4-level increase pursuant to U.S.S.G. §2A6.1(b)(4) because the offense resulted in a substantial disruption of government functions/service and a substantial expenditure of fund to respond to the offense. For the agency victims, the PSR calculated the base offense level as 6 pursuant to U.S.S.G. § 2B1.1(a)(2) along with a 10-level increase pursuant to U.S.S.G. § 2B1.1(b)(1)(F) because the loss amount of the offense was more than $150,000 but less than $250,000. The PSR also included a 2-level increase pursuant to U.S.S.G. § 2B1.1(b)(10)(B) because a substantial part of the scheme was committed from outside the United States and/or involved sophisticated means. The United States agrees that the calculations and enhancements set forth in the PSR are appropriate and supported by the evidence.

After grouping the offense levels, and applying a 4-level increase pursuant to U.S.S.G. § 3D1.4, the PSR calculated defendant's combined adjusted offense level as 28. With the two-level reduction pursuant to U.S.S.G. § 3E1.1(a) and given defendant's timely acceptance of

responsibility, the government moves the Court for a one-level reduction under U.S.S.G. § 3E1.1(b), which the Probation Office has appropriately included in its calculations. PSR ¶ 96.

The PSR calculated defendant's total offense level as 25. With defendant's criminal history category of 1, the resulting sentencing range is 57-71 months' imprisonment. The statutory maximum term of imprisonment is 60 months. PSR ¶ 132.

II. Section 3553(a) Factors

Applying the factors in 18 U.S.C. § 3553(a), the government submits that a sentence at the low end of defendant's guidelines range is appropriate, particularly given the nature and circumstances of the offense; defendant's relative role in the conspiracy; and the need for the sentence to reflect the seriousness of the offense, promote respect for the law, and afford adequate deterrence. For the reasons explained herein, the Government believes that Liverman's sentence should be significantly more than the 24 months' imprisonment received by Boggs to reflect his greater role in the conspiracy.

There is no dispute about the serious nature of defendant's offense. From at least in or around November 2015 to in or around February 2016, defendant conspired with others to break into U.S. government officials' online accounts and law enforcement databases. The group's objectives were to harass, pilfer law enforcement data to post online, and seek self-glory. Defendant and his co-conspirators crowed on Twitter of their exploits while hopscotching between victims in the fall and winter. They shared unlawfully obtained law enforcement information with online journalists who wrote about CWA. PSR Ex. 3 at 10. Their motives, in short, were in equal measure wreaking havoc and self-aggrandizement. In total, defendant and

his co-conspirators targeted more than 10 victims and caused more than $1.5 million in losses. Statement of Facts (SOF)[2] ¶ 4.

Other than the group's leader, a U.K.-based hacker in his mid-teens who went by "Cracka," Liverman's actions in furtherance of the conspiracy were the most involved of any other participant. Until his actions as part of the instant conspiracy, the defendant had attained a modicum of notoriety as part of a hacking collective that called itself "AnonSec." He utilized several pseudonymous online accounts that furthered his standing in the hacking world, including Twitter accounts @_D3F4ULT, @BASHTIEN_, and @SHIN0D4. SOF ¶ 2, PSR ¶ 42. While the world now knows that defendant created and controlled each of these accounts, for a time it seemed as though @_D3F4ULT was an administrator and leader of the much larger AnonSec group that included many other individuals, including @BASHTIEN_ and @SHIN0D4, as devoted followers. The defendant went to great lengths to perpetuate these frauds.

It is within this context that in October 2015, defendant congratulated Cracka in a private Twitter message for successfully gaining unauthorized access into Victim 1's online account, stating "[Victim 1] got bent lol." SOF ¶ 5, PSR ¶ 42. At the time, Victim 1 was a senior U.S. government official who worked and resided in the Eastern District of Virginia. With the publication of a New York Post article about his exploits, Cracka had attained the type of instant fame and notoriety that Liverman craved but which had so far escaped him. Cracka was receptive to Liverman's introduction, and thus bloomed a very successful pairing that would result in the online harassment of multiple victims and the instant conviction for defendant.

[2] ECF No. 54; text reproduced in PSR ¶ 42.

Liverman's role in the conspiracy grew significantly as time went on. On or about November 1, 2015, during a Jabber instant messaging conversation, Cracka informed Liverman that he had gained unauthorized access to Victim 2's account with Internet service provider Comcast. At the time, Victim 2 was a senior U.S. government official who worked for a federal law enforcement agency. Defendant replied to Cracka, "plz jack all [Victim 2's] shit haha." SOF ¶ 7, PSR ¶ 42. Defendant continued to encourage Cracka, suggesting that Cracka hack into Victim 2's government email account, stating: "if you could get into [Victim 2's] [U.S. Government Agency] acc im sure it would yield." Id. Later that day, defendant posted on his pseudonymous Facebook and Twitter accounts a screenshot of a document unlawfully obtained from Victim 2's online Comcast account.

The next day, however, Liverman chose to exponentially increase his role in the conspiracy by doing much more than just encouraging Cracka to continue targeting Victim 2: having obtained Victim 2's cellphone number from Cracka and after confirming that the number was legitimate, Liverman decided to engage in a form of constant harassment referred to as "phonebombing." Liverman paid an online service to automatically dial Victim 2's phone number once an hour, for 30 days, and leave a threatening recorded message. SOF ¶ 8, PSR ¶ 42. But Liverman was not done with Victim 2. He also decided to use a temporary email service to send the following text messages to Victim 2's cellphone:

> Listen here you fucking boomer, we will destroy your reputation.
>
> Just like [Victim 1 and another senior U.S. government official] … I guess you couldn't handle us jacking your Comcast ISP accounts too many times so you actually canceled your account! And telling me to "watch my back" wasn't a good idea lol How your slut wife [spouse first name]? **We will keep a close eye on your family, especially your son!**

SOF ¶ 7, PSR ¶ 42 (emphasis supplied). At the end of the text message, defendant linked to a photograph of Victim 2's son. Defendant sent Victim 2 the above harassing message multiple times. SOF ¶ 9, PSR ¶ 42. Defendant also solicited text messages and calls to Victim 2's cellphone number via his pseudonymous Facebook and Twitter accounts. SOF ¶ 11, PSR ¶ 42. Defendant bragged about his actions on behalf of the conspiracy to Cracka via Jabber instant messaging. SOF ¶ 10, PSR ¶ 42. In one of these conversations, the defendant suggested to Cracka, "if we could get [Victim 2] swatted that would be amazing." SOF ¶ 12, PSR ¶ 42. By "swatted," defendant was referring to the crime of placing hoax calls to an emergency service, such as a police department, to falsely report that an imminent or ongoing critical incident was occurring. This wouldn't be the last time that the defendant and Cracka would discuss swatting.

Liverman leveraged Cracka's superior social engineering skills to his own ends – namely, to cause disruption/fear through harassment and to continue to perpetrate his online fraud of being an administrator of a hacking group and a successful hacker himself. For example, on or about November 4, 2015, Cracka informed defendant that he had used Victim 2's official credentials to obtain unauthorized access to the Law Enforcement Enterprise Portal ("LEEP"), a U.S. government computer system for law enforcement agencies, intelligence groups, and criminal justice entities. SOF ¶ 13, PSR ¶ 42. With the apparent aim of perpetuating an online vendetta against law enforcement in the Miami area, the defendant asked Cracka if he could search LEEP for a list of officers in Miami. Shortly thereafter, Cracka sent the defendant a list of information Cracka had obtained through Victim 2's LEEP account – including names, phone numbers, and email addresses – relating to more than 80 police officers and law enforcement employees in the Miami area. Id. On or about January 21, 2016, the defendant uploaded this information to publicly accessible websites. Id.

Liverman also made targeting decisions for the conspiracy. For example, in December 2015, the conspiracy targeted Victim 3 and Victim 3's spouse in its hacking and phone-harassment scheme. At the time, Victim 3's spouse was a senior U.S. government official. SOF ¶ 14, PSR ¶ 42. On or about December 10, 2015, Liverman decided to target Victim 3 because "[s]he talks mad shit abt snowden." Id. Cracka subsequently obtained the cellphone number of Victim 3's spouse and used social engineering to gain unauthorized access to Victim 3's online Verizon account. However, Cracka encountered some difficulties with accessing that account, and asked defendant whether he wanted to try logging into the account. Defendant then used login credentials that he received from Cracka to make multiple attempts to gain unauthorized entry into Victim 3's online Verizon account. SOF ¶ 17, PSR ¶ 42. Liverman discussed with Cracka via Jabber instant messaging different ways of harassing Victim 3. Ultimately they decided to post a taunting message along with an image of the sign-in page for Victim 3's Verizon account that included the phrase "cracka_d3f4ult_bashtien_2015." SOF ¶ 18, PSR ¶ 42. At Cracka's request, Liverman placed calls to Victim 3's telephone numbers to confirm that they were legitimate numbers. Over the next few days, Cracka called Victim 3's spouse's cellphone and residential phone number multiple times with the intent to harass her. SOF ¶ 19, PSR ¶ 42.

Liverman also encouraged Cracka to target Victim 4 and expressed his desire to "phonebomb [Victim 4's] voicemail… and sms spam." SOF ¶ 21, PSR ¶ 42. At the time, Victim 4 was a senior U.S. government official who worked for a federal law enforcement agency. Liverman and Cracka had extensive conversations via Jabber instant messaging about different ways they could harass Victim 4 using the information they had unlawfully obtained from Victim 4's Comcast account. Ultimately, they decided to alter the Comcast account settings for Victim 4's home in the Eastern District of Virginia by, among other things, resetting Victim 4's account

password, causing certain movies to play on the cable box at Victim 4's house, and renaming Victim 4's cable boxes "[Victim 4] is a slut," "fuck the cia," "fuck the fbi," and "fuck you." SOF ¶ 22, PSR ¶ 42. But even those actions were not enough: Cracka uploaded Victim 4's home telephone call logs to a publicly accessible website and members of the conspiracy made at least one harassing phone call to Victim 4. SOF ¶ ¶ 22-23, PSR ¶ 42.

Liverman was also instrumental in the conspiracy's targeting of Victim 5 and Victim 5's spouse, including the harassment of these victims' daughter. At the time, Victim 5 was the CEO of a company with an office in the Eastern District of Virginia that provided, among other things, information technology services to government and private sector customers. SOF ¶ 24, PSR ¶ 42. As with prior victims, Liverman and Cracka discussed in detail various ways to harass Victim 5. Using unauthorized access to a Facebook account that belonged to Victim 5's spouse, the defendant and Cracka staged a Facebook conversation appearing to be between Victim 5's spouse and Joseph Markowicz, an account controlled by Liverman. In the conversation, Liverman stated "I see that daughter you got," and inserted a link to Victim 5's daughter's Facebook page. It was Liverman who publicized the conspiracy's exploit, posting a screen shot of the fake conversation on January 8, 2016 under the caption, "[Victim 5's company name] CEOs wife caught by @_d3f4ult supporting terrorist Junaid Hussain (TriCk) & admitting to incest." SOF ¶ 25, PSR ¶¶ 35, 42.

In late January 2016, Liverman encouraged Cracka to execute a swatting campaign against the Palm Beach County Sheriff's Office in Florida. After Cracka said he was going to swat a police department, Liverman encouraged him, writing "ayyyyyyy yolo fuck it" and "hopefully they will have a shootout and kill eachother." SOF ¶ 26, PSR ¶ 42. Cracka asked "shall i say i got bombs in the building?" to which Liverman responded "yeaaa that usually

works … nano thermite." Id. Cracka made the call and did exactly as Liverman suggested, claiming during the hoax call that there were bombs located in the Office's Belle Glade administrative building. The defendant and Cracka then exchanged online links to the unfolding press coverage of the hoax bomb-threat call. SOF ¶ 27, PSR ¶ 42.

Up until that time, the public notoriety that CWA had obtained through its exploits fell mostly on Cracka. Not to be outdone, however, in late January 2016, defendant falsely claimed on his pseudonymous Twitter account that he had successfully compromised computer systems belonging to the government agency NASA. SOF ¶ 28, PSR ¶ 42. Liverman used the Twitter account @OPNASADRONES – which he created and controlled – to claim that he had gained unauthorized access to sensitive NASA information, including hundreds of aircraft and radar videos, thousands of flight logs, and data on thousands of NASA employees. This "leaked" data was in fact either fake or publicly available. Id. NASA incurred $41,300 in investigating defendant's false computer intrusion claims. SOF ¶ 28, PSR ¶ ¶ 42, 45.

Defendant claims in his statement attached to the PSR that "even though it was never my idea, I willingly and actively conspired to social engineer the email accounts of multiple federal government employees' for various reasons. At the time, I thought my reasons were political and valid." PSR Ex. 1 at 1. Defendant's claims are belied by his actions throughout the course of his involvement in this conspiracy as detailed above. He joined the conspiracy in or around November 2015 to obtain online fame and notoriety. His role exponentially increased during the four months that he was an active participant in the conspiracy, going from a congratulatory email to becoming one of the conspiracy's principals who made targeting decisions on behalf of the conspiracy; he attempted to access victim's online accounts himself; he solicited and then published personal information about government employees; he made harassing phone calls,

sent threatening text messages and e-mails, and harassed members of victims' families with online threats. He did not engage in these activities for political reasons, but rather for amusement and self-aggrandizement which he sought to achieve through harassment and causing fear.

In the same statement, defendant baldly claims that "[t]his Court will never see me again." PSR Ex. 1 at 1. As with everything else relating to this defendant, such a statement has proven to be self-serving and false. Specifically, the Probation Office has determined that Liverman violated his conditions of release by committing new felonies, namely possession of cocaine and drug paraphernalia in late May 2017. See PSR ¶¶ 10-12; p. 30. In light of the above, the government submits that a paramount consideration for defendant's sentence is that it promotes respect for the law and sends a signal to others who might consider following his steps.

--The remainder of this page intentionally left blank.--

CONCLUSION

For the reasons stated above, the government respectfully submits that a sentence at the low end of the Guidelines range of 57-71 months is sufficient but not greater than necessary under 18 U.S.C. § 3553(a). The government also respectfully requests a three-year term of supervised release, as well as the entry of a restitution order for $145,903.59 – payable to victims whose names will be submitted under seal – to which defendant and co-defendant Boggs are jointly and severally liable in the amount of $104,144.64.

Respectfully submitted,

Dana J. Boente
United States Attorney

By: /s/
Joseph V. Longobardo
Special Assistant United States Attorney (LT)

Maya D. Song
Jay V. Prabhu
Assistant United States Attorneys

United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Tel: (703) 299-3700
Fax: (703) 299-3981
maya.song@usdoj.gov
jay.prabhu@usdoj.gov
joseph.longobardo@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on July 21, 2017, I will electronically file the foregoing with the Clerk of Court using the CM/ECF system, which will automatically generate a Notice of Electronic Filing to counsel of record for defendant Justin Gray Liverman.

By: /s/

Joseph V. Longobardo
Special Assistant United States Attorney (LT)
United States Attorney's Office
Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, Virginia 22314
Ph: (703) 299-3700
Fax: (703) 299-3981
joseph.longobardo@usdoj.gov